System Services CSCI

Access Control and Security CSC

Thor Design Panel 2/3 Review

84K00510-030

December 2, 1997

Tom Nguyen

1. Access Control and Security CSC

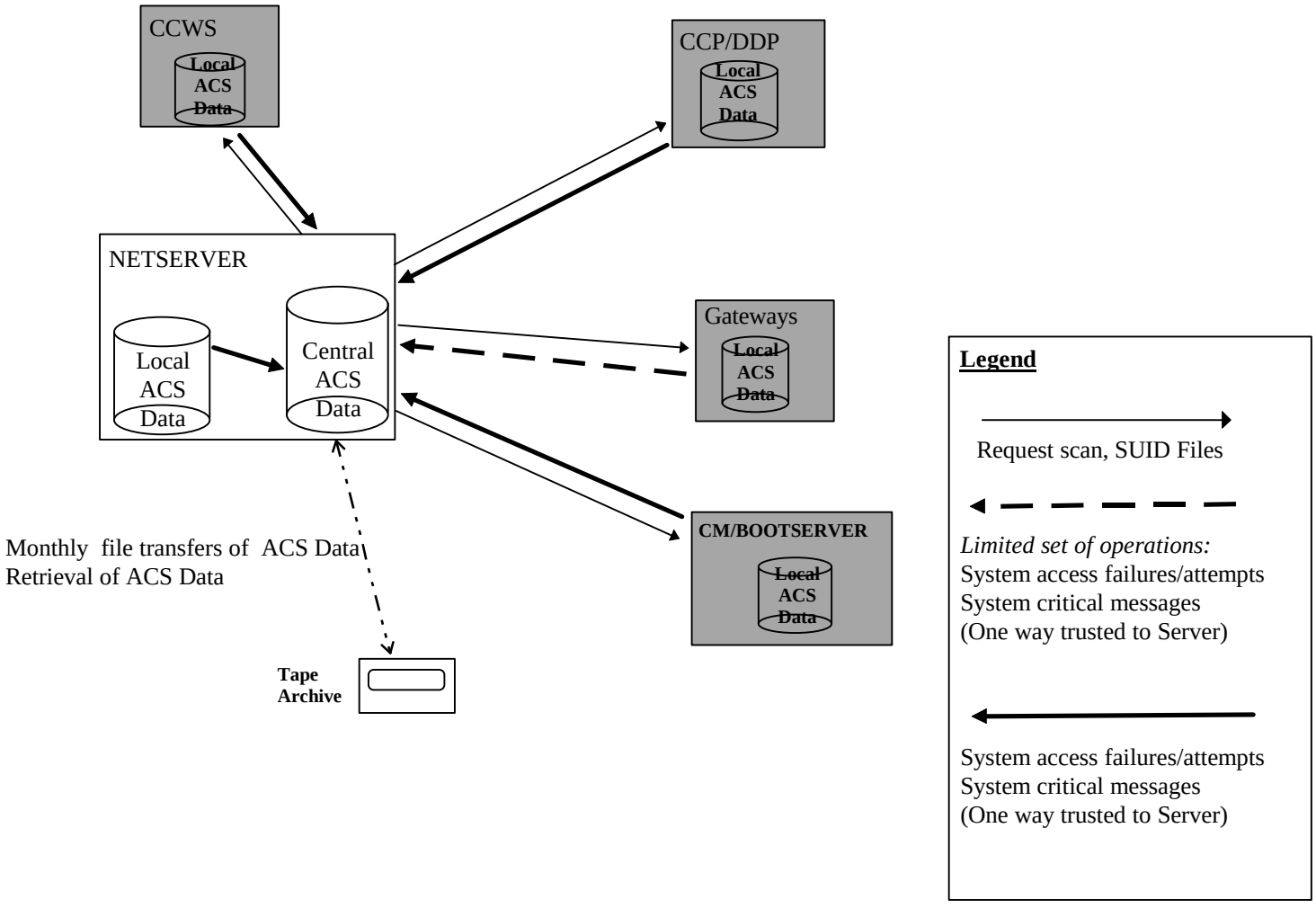
1.1 Access Control and Security CSC Introduction

1.1.1 Access Control and Security CSC Overview

Access Control & Security will provide access control and audit policies for CLCS. These policies will address system access, system file integrity, user security, and auditing requirements. The boundaries of the Access Control & Security measurement are the network connection point of the individual system and it's internal configuration (i.e. Network traffic/data is not considered as part of this CSC).

The Access Control & Security CSC are the software components that applies each machine, and provides control and auditing using standard built-in COTS OS procedures and features.

Access Control & Security CSC diagram:



1.1.2 Access Control and Security CSC Operational Description

Access Control & Security (ACS) can be divided into server and clients. The server is a secure machine used for monitoring, logging, and auditing of all client systems. The server shall maintain the central ACS data. The server and clients will be connected on the homogenous network. The clients will trust and send all ACS data to the server.

The server will periodically transfer the central ACS data to tape for storage and future retrieval if necessary. In the operational environment this storage will be a local tape drive with a minimum capacity as specified in 1.2.1. However, in the development environment this storage may be via the existing Auspex File Server (or designated equivalent) where ACS data will reside and backup with normal daily system backup functions maintained by the development team (i.e. System Services - OS group).

1.2 Access Control and Security CSC Specifications

1.2.1 Access Control and Security CSC Ground rules

The following assumptions will apply

- OPS/CM will provide the requirements and implementation of the no user login capability
- OS will provide COTS security tools
- Network services will provide firewall security including network scanning/monitoring/filtering/etc.
- Central ACS data is not expected to exceed a maximum of 1GB of data per month to be transferred to tape (assuming maximum of 50 CCWS).

1.2.2 Access Control and Security CSC Functional Requirements

Functional requirements will be divided into the following categories:

System data integrity:

1. All ACS data will be automatically stored and archived.

2. ACS will provide the capability to retrieve archived ACS data.

3. All systems which are to be “secured” will have a one way trust relationship to the centralized ACS data location.

System auditing:

4. All clients and hosts will have a security banner prescribed by NASA for government computers when a login prompt is presented.

5. ACS will monitor/record all client login attempts/failures defined for the operational and developments sets.

6. ACS clients will log system related warning and critical messages.

7. ACS will protect/limit/log/monitor Super User[1] access/usage on all clients.

8. ACS will define/limit/log/monitor trusted[2] hosts/users to each client system.

9. ACS will examine/log/monitor all SUID programs/files (including system and user files) on all clients. (Scans can be done periodically and be executed unobtrusively at low priority)

System security:

10. ACS will disable unnecessary accounts (i.e. demo, games, nobody, etc) on all clients.

11. ACS will disable all unnecessary network services (i.e. sendmail, httpd, tftpd, finger, programs/daemons) on all clients.

12. ACS will verify exported (shared) filesystems for security (i. e. writable by everyone) on all clients.

1.2.3 Access Control and Security CSC Performance Requirements

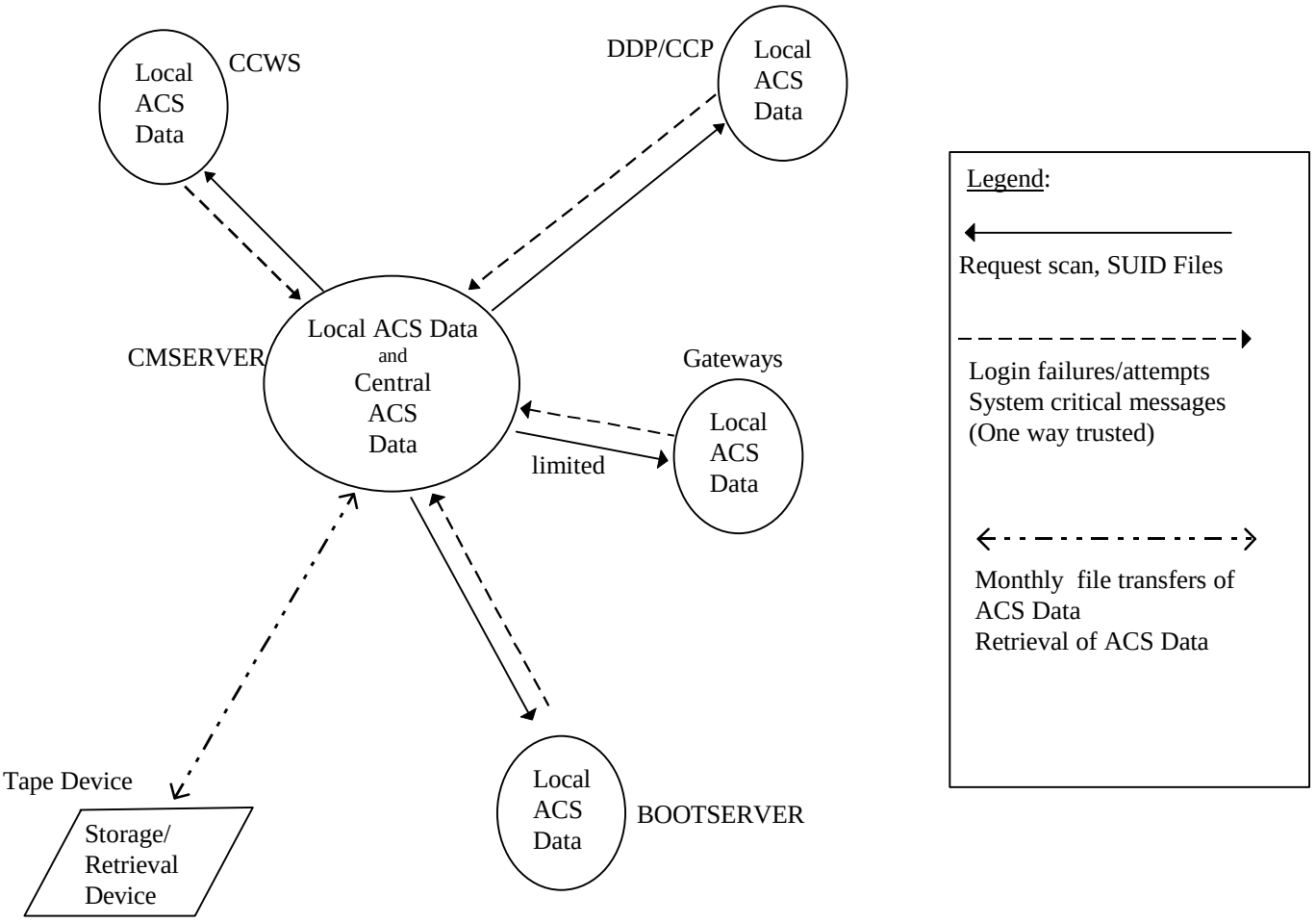
No specific requirements for Thor.

1 - Super User is a user with extra privileges to execute/access system commands (ID and privileges equivalent to "root").

2 - trusted host/user is a host/user that can execute/access the system commands and does not require authentication.

1.2.4 Access Control and Security CSC Interfaces Data Flow Diagrams

DFD Diagram:



Hardware Diagram: